SERVICE GRAPH BASED VULNERABILITY ANALYSIS FRAME WORK FOR BUSINESS INTELLIGENCE USING STATE TRANSITIONAL MATRIX

S. Senthil Kumar[1], *M.Prabhakaran*[2]

ABSTRACT

Growing internet technology supports the business activities to be performed through online, where there is a mutual growth of vulnerabilities and internet threats. The performance of business applications has more threats from malicious users and internet attacks. The problem of vulnerability has been studied well in the literature and we propose a new service graph based approach for vulnerability analysis to support business intelligence. In any service oriented architecture or application, each service has its own states and each has some priorities according to their end state. The proposed approach constructs such a graph for distinct services and assigns states of service as nodes and links them from possible transitions. The approach maintains set of values for each state specifying the loyalty value of the state from the previous state. Then the proposed method constructs a state transitional matrix for each of the log present in the web log using the values available in the constructed graph. Finally we compute a cumulative vulnerability score, which specifies the trustworthy of the user. The proposed approach has produced efficient results and has reduces the overall time complexity.

***Keywords** - Business Intelligence, Service Oriented Architecture, Vulnerability Analysis.*

I. INTRODUCTION

The growth of internet technology paves the huge gate for the e-commerce to be performed easily. The people purchases and shops many things easily through the internet. How they perform shopping through internet is through the services available. There are services for everything like payment, shopping and etc. Generally these services are loosely coupled and have no strong bound between them.

The business organizations maintain various information's about the corporate as well as individual or customers. The amount of information is vast in volume and huge in important, because they have the responsibility to maintain all those information for them in secure manner. The kind of risk arises in maintaining the user information's are due to variety of malicious threats which can be generated by dedicated groups or individual. What the threatening groups can do is, they can steal the information and initiate some attacks. For example, if the organization is supporting online shopping, a genuine user will provide his account details like credit card no, to the online interface. So that the card no will be

[1]Research Scholar, Department of Computer Science, Karpagam University, Coimbatore, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamil Nadu, India

validated through some other interfaces from the organization. Later the user will be asked for transaction passwords and confirmations. What happens when a malicious user catches the secret information is, the malicious user can do some malformed activities and he can shop some goods on behalf of the original user and pay from the steal account. Similarly, a malicious user can perform many ways of threats.

In a service oriented architecture , there are services for everything. The user will not no anything happening at the back of service. What the user has to do is, what the service needs and he has to provide that information to the service. The user will be unaware of the process happening in the background. While performing shopping through online, the user has to pay the amount through some of the gateway provided by the shopping company. The trustworthy of the gateway does not know to the user and he simply provide information whatever it asks. What will happen is the minimum user information may be caught by some malicious user and could be used to perform malicious activity later by providing maximum information but lags with little information to complete the transaction. This little information safeguards the user details and restrict the malicious user to perform any attacks.

The vulnerability has to be measured based on the effect the threat makes to the business system. For example, if a malicious user generates anonymous request through a service provided by the business system, then vulnerability of the service or the user has to be measured based on the frequency of access and how much the service access damages the business service and data. Once the pattern of malicious access or threat has been identified then , the business system has to modify the protocol of access to override the malicious access or vulnerable pattern.

II.RELATED WORKS

There are various approaches has been discussed earlier for the analysis of vulnerability and we discuss few of them here around the problem statement.

A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis [3], proposes a maximum-flow-based complex network approach for the analysis of the vulnerability of power systems. A new centrality index is proposed, taking into consideration the maximum flow from the source (generator) nodes to the sink (load) nodes, for assessing the network. The Max-Flow Min-Cut Theorem, also known as Ford-Fulkerson Theorem, is used for evaluating the capacity of links. The proposed methodology is then used to identify vulnerable lines of the IEEE 118 bus system and its effectiveness is demonstrated through simulation studies.

Vulnerability Analysis of Wide Area Measurement System in the Smart Grid [4], performs a comprehensive analysis of security issues with a wide area measurement system is presented and the research efforts required to be taken are identified. Moreover, the effect of communication failure on a PMU installed system has been presented using integer linear programming

The Research on Network Vulnerability Analysis Methods [9], summarized the popular vulnerability Analysis Methods in the field of computer network security. This paper also described and compared these methods. Then this paper introduced the Vulnerability analysis methods for communication network, command & control network, mobile ad hoc network and satellite network. At last, the shortage of current research on satellite network vulnerability was analyzed and the next research idea was proposed.

VULCAN: Vulnerability Assessment Framework for Cloud Computing [10], propose a novel vulnerability assessment framework for cloud computing systems. We have designed and developed a prototype of our framework. We also present the design and development of our framework with some use cases.

Ranking Attacks Based on Vulnerability Analysis [13], provide a set of security metrics to rank attacks based on vulnerability analysis. The vulnerability information is retrieved from a vulnerability management ontology, which integrates commonly used standards like CVE, CWE, CVSS, and CAPEC. Among the benefits of ranking attacks through the method proposed here are: a more effective mitigation or prevention of attack patterns against systems, a better foundation to test software products, and a better understanding of vulnerabilities and attacks.

Software vulnerability analysis framework based on uniform intermediate representation [14], presents a static analysis framework based on uniform intermediate representation to detect software vulnerabilities, and we have implemented an analysis tool called Melon based on the Microsoft Phoenix. We evaluate the effectiveness of Melon through a number of testing, and the experimental results show that it can effectively validate and analyze software vulnerabilities.

All the above approaches are struggle with identifying new kind of vulnerability and we propose a naval approach to find the new pattern of vulnerable attack.

III. Proposed Method

The proposed method consist of Four stages namely Preprocessing, Service Graph Construction, Transitional Matrix generation, Vulnerability Analysis.

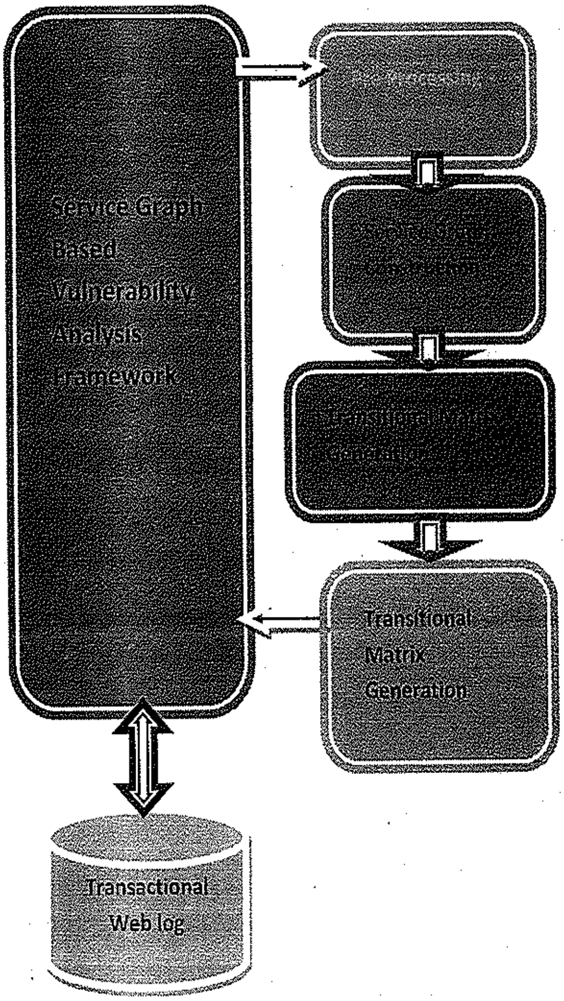

Service Graph Based Vulnerability Analysis Framework
Transitional Matrix Generation
Transactional Web log

Figure1: Proposed System Architecture

3.1 Preprocessing :

At the preprocessing stage from the web log , distinct and unique attributes of the transaction are identifies. The noise logs which does not have any value for the attribute is identified. The identified noisy logs are removed from the transactional data set Ts. The transaction log contains information about the time , url, address and other user information , service accessed and their states are identified to form the log.

```
Algorithm:

Input: Transactional Web log Twl

Output: Preprocessed TWL.

Step1: for each transaction Tl from Twl

Identify distinct Attributes and add to attribute list Al.

Al = $\int_{1}^{N} (\Sigma Tl(i)(Attr))\nexists Al)$
end.
Step2 : for each Transactional log  Tl from Twl

if  $\int_{1}^{N} = \square\ Tl\ (i)(Attr))\nexists Al)\square$ then
        Twl = Twl          og.
                      $\cap Tl$
        End

Step 4 : stop.
```

3.2 Service Graph Construction:

At this stage each distinct service and their states are identified. The proposed method has assigned proactive values for each state and for each transaction belongs to the service identified; the transaction logs are split into groups. From the separated group of transaction, and states of the service identified, we construct a graph using the service name and for each state identified we create a node and engage them with other nodes of the graph according to the state flow. From the log list, each service states are identified and the number states followed at a single service is calculated and assigned to the state nodes.

```
Algorithm :

Input : Transaction log Twl.

Output : Service Graph:

Step1: Identify set of distinct services S =

    $\int_{1}^{N}\sum s \ni s$

Step 2 : for each service $S_i$ from S

        Identify set of states St = $\Sigma\mu\times S_{i(service)}$   $\sum St$

        Create a graph G =

Assign state values to the nodes of G.

        end.

Step3: For each service Si

        Identify set of logs accessed the service $S_i$

        Identify set of states followed.

        Increment the state counter present in the node.

        end.

Step4: stop.
```

3.3 State Transitional Matrix Computation:

The state transitional matrix is compute using generated graph. The state transitional matrix consists of various service names and states and completeness values for each state and their finishing stage. From the graph constructed, for each service available a row will be generated. In the service row, each values of the service , state , count and their trust values are computed to form the matrix. The final status of the service access has three values namely success, Fraudulent, NotSuccess.

Algorithm:

```
Input: Service Graph SG.
Output: State Transitional matrix STM.
Step1: read each service graph sg
    For each transaction from Ts
        Compute the service, status, count of service, finishing status count.
        $\int_{1}^{N} \sum Sg(i).\ status,\ count,\ trust\ values.\ finishing\ stage.$
        STM(i)=
    End.,
Step2: Stop.
```

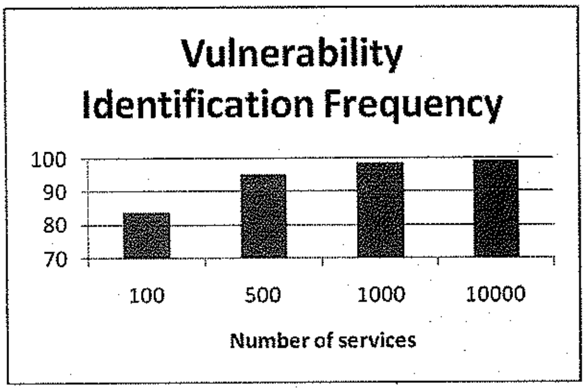
3.4 Vulnerability Analysis :

At this phase, for each combination of status of service from the initial stage we compute the vulnerability score, which showing the frequency of vulnerability could occur. We have all the details available at the state transitional matrix and from the matrix available we compute the vulnerability score for each of the transaction pattern from the transaction log. IF the vulnerability score is higher than the threshold then the transaction is considered as vulnerable transaction and will be removed.

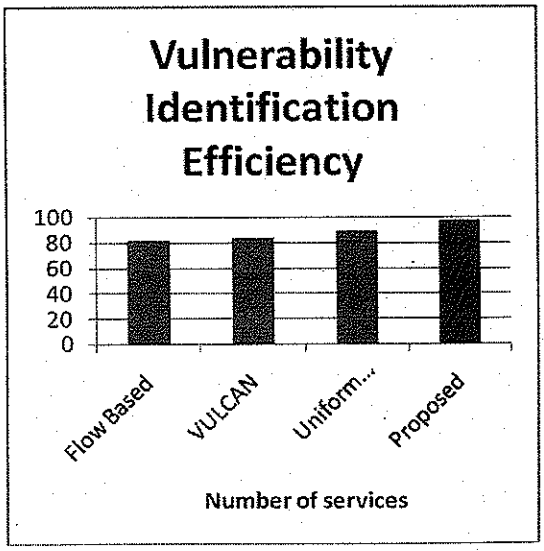
IV. Results and Discussion

The proposed Service Graph based vulnerability analysis framework has produced better results in identifying the malicious threats and network threats which happens in different business environment also in other transactional fields.

Table1: shows the frequency of identifying vulnerability.



The table 1, shows the vulnerability identification frequency, it shows the frequency raises with number of service logs.



Graph 2: Comparison of efficiency of different methods

The graph2, shows the efficiency of vulnerability identification, and it shows that the proposed approach has produced more efficiency in identification process.

V. CONCLUSION:

We proposed a vulnerability analysis framework which uses the web log traces to preprocess and extracted the necessary features to generate service graph. The service graph has all the details about the transaction like url, address, service name, set of state followed and etc. We compute a state transitional matrix which represent the pattern of transaction followed in the log and their vulnerability score to identify the vulnerable pattern and transactions. The proposed approach has produced efficient results with less time complexity.

References

[1] *Unclassified Statement for the Record on the World wide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence James* R. Clapper Director of National Intelligence January 31, 2012.

[2] *"Towards a new stage in the bi-regional partnership: innovation and technology for sustainable development and social inclusion"* MADRID ACTION PLAN 2010-2012.

[3] Dwivedi A, A Maximum-Flow-Based Complex *Network Approach for Power System Vulnerability Analysis,* Ieee Transaction on industrial informatics volume 9, issue 1, pp 81-88, 2013.

[4] M. Rihan, M. Ahmad and M. Beg, *"Vulnerability Analysis of Wide Area Measurement System in the Smart Grid,"* Smart Grid and Renewable Energy, Vol. 4 No. 6A, 2013, pp. 1-7.

[5] Walnerstrom c.j., *Vulnerability Analysis of Power Distribution Systems for Cost-Effective Resource Allocation,* ieee transactions on power systems , vol 27, issue 1, pp 224-232, 2012.

[6] Yang hang, *A Framework of Business Intelligence-Driven Data Mining for E-business,* NCM, pp 1964-1970,2009.

[7] Ciabanu V, *A Distributed Approach to Business Intelligence Systems Synchronization, Symbolic and Numeric Algorithms for Scientific Computing* (SYNASC),pp 581-595, 2010.

[8]. Hossain Shahriar, *Mitigation of Program Security Vulnerabilities: Approaches and Challenges,* ACM, 2014.

[9]. Yong Wang, *Research of Network Vulnerability Analysis Based on Attack Capability Transfer, IEEE international conference on computer and information technology,* pp:38-44, 2012.

[10] Shiguo Sun, *The Research on Network Vulnerability Analysis Methods [8], International conference* on intelligent system design and engineering application, pp:593-597, 2012.

[11] Kamongi P, VULCAN: *Vulnerability Assessment Framework for Cloud Computing,* International conference on software security and reliability, pp:218-226, 2013.

[12] Chopade, *Structural and functional vulnerability analysis for survivability of Smart Grid and SCADA network under severe emergencies and WMD attacks,* International conference on technologies for homeland security, pp:99-105, 2013

[13]. Ju An Wang, *Ranking Attacks Based on Vulnerability Analysis,* Hawaii, International conference on System Sciences, pp:1-10, 2010.

[14]. Jun Xu, Software *vulnerability analysis framework based on uniform intermediate representation, International conference* on software technology and engineering, vol.1, pp:356,361,2010.

Author's Biography

S.Senthil Kumar, is working as Business Intelligence Data Analyst in IT Security Analytics team in Investment bank. He completed his MCA (Mater of computer Applications) in Bharathidasan University and Mphil(CS) from Vinayaka Missions University . His research area of interest in "MULTI MODEL TIME VARIANT VULNERABILITY ANALYSIS FOR BUSINESS INTELLIGENCE SUPPORT".

Dr. M Prabhakaran, is working as Assistant Professor, Department of Computer Science Government Arts College, Ariyalur, Tamil Nadu. He completed his M.Sc(CS) from Bharathidasan University, ME (CS) & M.Phil (CS) from Vinayaka Mission's University and Phd(CS) from Vinayaka Mission's Unversity.He has more than 16 years of experience in his academic. He is supervising a lot of PhD Theses.He extends his guidence for the research activity by gving support for his fellow candidates. His research is focused on Image Processing, Data Mining, and Network Security.